IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a
California Corporation,

Plaintiff and
Counterclaim-Defendant,

v.

INTERNET SECURITY SYSTEMS,
INC., a Delaware corporation, INTERNET
SECURITY SYSTEMS, INC., a Georgia
Corporation, and SYMANTEC
CORPORATION, a Delaware corporation,

Defendants and
Counterclaim- Plaintiffs.

Civil Action No. 04-CV-1199 (SLR)

DECLARATION OF L. TODD HEBERLEIN

I, L. Todd Heberlein, declare that:

1. I make this declaration of my own personal knowledge. If called to testify as to the truth of the matters stated herein, I could and would do so competently.

2. I am the President of Net Squared, Inc.

3. I have been retained by counsel for Symantec Corporation as an expert witness in this action.

4. I have worked on a number of different network intrusion detection systems developed at UC Davis, including the Network Security Monitor (NSM) and the Distributed Intrusion Detection System (DIDS). Both NSM and DIDS analyzed, among other things, network packet volume and network connections (including the network packets involved in establishing and severing a network connection).

5. While developing NSM and DIDS at the University of California at Davis, one of our primary goals, especially as an academic institution, was to share the results of

our research with the public. To that end, members of the NSM and DIDS teams—including myself—published several papers and theses on NSM and DIDS. We also distributed source code to users outside of UC Davis, and provided technical support to those users. Because our work was funded in part by government agencies, we also delivered source code to those agencies funding our work.

NSM

6. I was the primary developer of the Network Security Monitor (NSM), as described in L.T. Heberlein, G.V. Dias, K.N. Levitt, B. Mukerhee, J. Wood, and D. Wolber, "A Network Security Monitor," Proc. IEEE Symp. Research in Security and Privacy, pp 296-304 (May 1990). The NSM processed network packets and applied anomaly and signature detection techniques to detect intrusive activity. The work began in 1988, and we published numerous papers describing the work in 1990, 1991, and 1994.

7. By the mid-1990s, the NSM had been in use by numerous organizations, including UC Davis, the Air Force, the Department of Energy, NASA, UC Santa Cruz, the Pentagon, the CIAC group at Livermore, Galaxy, the Defense Information Systems Agency (DISA), Wright Patterson Air Force Base, and the Department of Justice.

8. From at least as early as the beginning part of 1990 until 1993, NSM was in use at the Security Lab in the Division of Computer Science[1] at UC Davis. This use of NSM at the Security Lab was described in numerous publications, including my 1991 masters thesis, "Towards Detecting Intrusions in a Networked Environment." In my thesis, I devoted an entire chapter to my use of NSM on the Electrical Engineering and Computer Science LAN for a period of around three months. As I describe in my thesis,

[1] At this point in time, Computer Science was a Division under the Department of Electrical Engineering.

NSM detected 400 intrusive connections during that time. Several students and faculty members had access to the Security Lab during the time periods that NSM was in use. No one was made to sign a non-disclosure agreement, nor was there an expectation that the use of NSM at the Lab be kept secret.

9. By October 1991, NSM was also in use at UC Santa Cruz. The personnel at UC Santa Cruz used NSM to work with the Federal Bureau of Investigation to track an attacker who had broken into several sites.

10. Typically the NSM software was distributed to potential users as source code, a common practice for distributing UNIX software at the time. When I gave the source code to a third party, I realized that the third party would often share the code with other groups. For example, I know that Dan Teal, who at the time was affiliated with the Air Force, gave the code for NSM to several people; I know this because I received feedback from users who had received the NSM code from Mr. Teal. Likewise, I understand that the Army received a copy of the NSM code from Lawrence Livermore National Laboratory.

11. Several intrusion detections systems, such as the Network Intrusion Detector (NID) and the Automatic Security Incident Measurement (ASIM), were derived from the source code to NSM. By 1997, ASIM was widely deployed throughout the Air Force.

DIDS

12. I also worked on the Distributed Intrusion Detection System (DIDS), as described in Steven Snapp et al., "Intrusion Detection Systems (IDS): A Survey of Existing Systems and A Proposed Distributed IDS Architecture" (February 1991) and S.R. Snapp, J. Brentano, G.V. Dias, L.T. Heberlein, C. Ho, K.N. Levitt, B. Mukherjee,

(with S.E. Smaha, T. Grance, D.M. Teal, D.L. Mansur), "DIDS -- Motivation, Architecture, and an Early Prototype" Proc. 14th National Computer Security Conference, Washington, DC, Oct. 1991, pp. 167-176. DIDS was a distributed intrusion detection system that include LAN Monitors (which were based extensively on the source code for NSM), Host Monitors (which monitored activity on individual host computers), and a Director. Both the LAN and Host Monitors communicated bi-directionally with the Director.

13. From approximately 1991 to October 1992, DIDS was installed and in use at the Security Lab in the Division of Computer Science at UC Davis. During this time, around 20 individuals—including undergraduate students, graduate students, and faculty—had access to the lab. There were no confidentiality obligations imposed on the users of the Security Lab regarding the use of DIDS at the Lab: no one was made to sign a nondisclosure agreement, nor was there any expectation that the use of DIDS be kept secret. Students and faculty were free to publish such papers and theses relating to the use of DIDS at the Lab, without those papers and theses being cleared prior to publication by any of the government agencies providing funding for the work on DIDS (although, typically the sponsors were listed as co-authors on papers).

14. Beginning in early 1992, DIDS was also in use at Lawrence Livermore National Laboratory (Livermore). DIDS software successfully detected a successful attack into Lawrence Livermore National Laboratory computers. Several employees at Livermore had access to the DIDS installation. These employees were not made to sign non-disclosure agreements regarding their observations of the use of DIDS, nor were these employees expected to keep secret the use of DIDS at Livermore.

15. DIDS was also used by the Air Force. During 1991 or 1992, I personally

helped install DIDS at Kelly Air Force Base in San Antonio, Texas. Later, in 1994, I learned that the Air Force had installed DIDS on 133 different computers.

16. In October 1992, I participated in giving a demonstration of DIDS at the annual National Computer Security Conference (NCSC). At the conference, we gave a two to three day demonstration of DIDS. We set up a network of computers and installed DIDS on that network to monitor those computers. We demonstrated how DIDS could detect attacks on the network in real-time and how DIDS could track users as they logged in from one computer to another. On the last day of the demonstration, we allowed conference attendees to participate in the demonstration themselves in real-time. Any conference attendee was allowed to sit down at various computers in our demonstration network and launch various attacks, all while watching DIDS detect these attacks in real-time.

17. There were no obligations of confidentiality imposed upon either the attendees who watched the demonstration or the attendees who participated in the demonstration. No attendee was made to sign a non-disclosure agreement, nor was there any expectation that the attendees keep secret their observation of the demo or their participation in the demo. Our intent in conducting the demonstration was to share the details of DIDS to members of the public.

18. There were also efforts to commercially exploit the DIDS source code. In 1993, the Air Force awarded Trident Data Systems a contract to continue work on DIDS. Trident was a private for-profit company that sought to productize DIDS and expand the deployment of DIDS throughout the Air Force. We delivered the DIDS source code to Trident.

19. While in the process of preparing this declaration, I came across a series of

tape archives (magnetic computer tapes) created in the early 1990s. While, I did not then know contents of these archives, some of them were labeled "DIDS." Since I do not have access to a device that can read these magnetic computer tapes, I provided these tape archives to counsel for Symantec, who had these tape archives extracted for my review. Upon review, these archives contain source code for DIDS and NSM at different points in time, all prior to July 1993. Furthermore, while in the process of preparing this declaration, I came across a small box of 35 mm slides containing screenshots of DIDS in operation in September 1991. I have attached copies of these slides to this declaration as Exhibit A. Furthermore, while in the process for preparing this declaration, I came across another small box of 35 mm slides containing slides presented by myself and others from UC Davis at the 1992 National Computer Security Conference. I have attached copies of these slides to this declaration as Exhibit B.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge.

Signed on June 29, 2006.

L. Todd Heberlein

L. Todd Heberlein

CERTIFICATE OF SERVICE

I hereby certify that on the 30th day of June, 2006, I electronically filed the foregoing document, **DECLARATION OF TODD HEBERLEIN,** with the Clerk of the Court using CM/ECF which will send notification of such filing to the following:

John F. Horvath, Esq.
Fish & Richardson, P.C.
919 North Market Street, Suite 1100
Wilmington, DE 19801

Richard L. Horwitz, Esq.
David E. Moore, Esq.
Potter Anderson & Corroon LLP
Hercules Plaza
1313 North Market Street, 6th Floor
Wilmington, DE 19801

Additionally, I hereby certify that on the 30th day of June, 2006, the foregoing document was served via email and by Federal Express on the following non-registered participants:

Howard G. Pollack, Esq.
Michael J. Curley, Esq.
Fish & Richardson
500 Arguello Street, Suite 500
Redwood City, CA 94063
650.839.5070

Holmes Hawkins, III, Esq.
King & Spalding
191 Peachtree St.
Atlanta, GA 30303
404.572.4600

Theresa Moehlman, Esq.
King & Spalding LLP
1185 Avenue of the Americas
New York, NY 10036-4003
212.556.2100

/s/ Richard K. Herrmann
Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
Morris, James, Hitchens & Williams LLP
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
(302) 888-6800
rherrmann@morrisjames.com
mmatterer@morrisjames.com
Counsel for Symantec Corporation